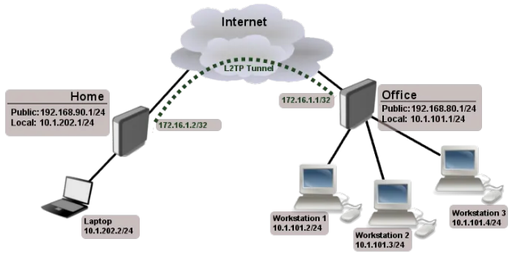
나무위키

가상 사설망

최근 수정 시각: 2026-08-16 05:04:33

분류:가상 사설망



L2TP를 이용한 VPN 접속 예[1]

목차

1. 개요
2. 용어 정리
3. 사용 목적
   3.1. 사설망(인트라넷) 구축
   3.2. 콘텐츠 접속 우회
   3.3. 적절한 서버 위치 선정으로 인한 인터넷 속도 향상
4. VPN으로 오해하는 것들
   4.1. 패킷 변조 애플리케이션
   4.2. 프록시 서버
5. 보안성
   5.1. 프로토콜상 익명성이 보호되는가?
   5.2. 해킹이 불가능한가?
   5.3. 이용자 로그 제공?
6. VPN 구축 및 이용
   6.1. 사설망(인트라넷) 구축 목적
      6.1.1. VPN 장비
      6.1.2. VPN 서비스
   6.2. IP 우회 목적
      6.2.1. 무료 VPN
      6.2.2. 유료 VPN
      6.2.3. 웹서핑 시 프라이버시 지키기
      6.2.4. 토렌트 사용 시 프라이버시 지키기
7. 다양한 분야에서의 활용
   7.1. 오락실에서의 이용
   7.2. 온라인 게임에서의 이용
      7.2.1. 게임용 VPN 서비스
8. 프로토콜
9. 구축용 소프트웨어
10. 연결 방법
11. 장점
12. 단점
13. 악용
   13.1. 스팸, 위키 반달 등 악용
   13.2. 사기에 활용
   13.3. 비방성으로 악용
   13.4. 비정상적인 가격으로 제품 우회 구매
   13.5. 그 외
14. 기타
15. 같이 보기

1. 개요

Virtual **P**rivate **N**etwork(VPN), 가상 사설망

터널링을 통해 만들어지는 가상 사설 통신망.

2. 용어 정리

- 사설망과 공중망
  가상사설망에서 사설망(私設網, Private Network)이란 개인이나 특정 기업이 사적인 목적을 위해 전용 회선을 설치하고 사설 IP 주소를 부여하여 만든 인트라넷이다. 반대로 공중망(公衆網, Public Network)이란 모두가 이용할 수 있는 네트워크, 주로 인터넷을 의미한다.

- 가상(Virtual)의 의미
  인트라넷을 구축할 때는 보통 해당되는 컴퓨터만 연결해서 제3자가 함부로 접근하지 못하게 만든다. 그러나 망의 규모가 커지면 커지거나 장거리로 구축해야 한다면 전용선 구축 비용이 크게 부담이 된다. 따라서 기존의 인터넷(공중망)을 이용하지만 대신 패킷을 아무도 볼 수 없도록 암호화하여 전송하여 가상의 인트라넷처럼 사용하는 방식을 가상 사설망이라고 부른다.

- VPN 라우터
  인터넷(공중망)에만 연결된 단말기는 인트라넷에 접근할 수는 없다. 왜냐하면 망이 완전히 분리되어 있기 때문인데[2], 이를 이어주는 브릿지 같은 역할을 하는 것이 VPN 라우터다. VPN 라우터는 해당 단말기가 마치 인트라넷에 연결된 것처럼 단말기와 인트라넷 사이를 중계하는 역할을 수행하게 된다. 따라서 단말기는 인터넷과 인트라넷을 동시에 사용할 수 있는 상태가 되는 것인데, 단말기를 통해 인트라넷에 접속한 경로를 보면 인터넷/인트라넷 상에는 전부 라우터까지의 접속만 수행한 것으로 보인다. 알기 쉽게 표현하자면 컴퓨터에서 집 공유기에 연결한 것과 논리적으로 같은 구조라고 생각하면 된다.

- 터널링
  인터넷 단말기에서 라우터에 VPN 프로토콜 중 하나를 이용하여 연결을 시도한다. 연결 시에는 비밀번호 같은 자격 증명이 필요한 경우가 보통이며 성공시에는 단말기와 VPN 라우터 사이에 암호화된 연결이 형성되게 된다. 이를 터널링이라고 한다.

3. 사용 목적

3.1. 사설망(인트라넷) 구축

가상 사설망은 이름을 보면 알 수 있듯이, 원래는 **공중망(인터넷)을 통해 가상의 사설망(인트라넷)을 구축**하기 위해서 개발되었다.

예를 들어서, 어떤 회사가 본사와 지사 간에 사내 네트워크(인트라넷)을 공유하려고 한다고 해 보자. 옛날에는 이를 위해 본사와 지사를 잇는 전용회선을 설치해야 했는데, 이는 비용이 매우 많이 드는 일이었다. 하지만 VPN의 등장 이후에는 그냥 본사와 지사에 VPN 라우터를 놓고, 이들을 각각 공중망(인터넷)에 연결한 뒤 그 위에서 VPN 연결을 구성하기만 하면, 전용회선 없이도 본사와 지사 간에 동일한 사내망을 공유할 수 있게 되었다. 이러한 종류의 VPN을 Site-to-site VPN이라고 한다.

또 재택근무를 하거나 출장을 나간 직장인 등이 인터넷에 연결된 자신의 컴퓨터로 사내망에 접속하기 위해 VPN을 사용하기도 한다. 이러한 종류의 VPN은 Remote Access VPN이라고 한다.

네트워크 자체가 분리되어 있어 보안이 유지된다는 전용회선의 특징을 보안이 보장되지 않는 공중망(인터넷) 위에서 구현하기 위해, VPN을 통해 오가는 트래픽은 보통 암호화를 거친다. 또 허용된 사용자만 접속할 수 있도록, 접속할 때 인증서 제출이나 로그인 등 인증을 요구하도록 구현된다.

이처럼 저렴한 인터넷 연결만 가지고도 비싼 전용회선을 깔아 사설망을 구축한 것과 비슷한 효과[3]를 낼 수 있기 때문에, VPN은 오락실의 온라인 대전용 네트워크부터 은행과 ATM 간의 네트워크에 이르기까지, 다양한 인트라넷 구축에 사용되고 있다.

3.2. 콘텐츠 접속 우회

이처럼 원래 "가상"의 "사설망"을 구축하기 위해 만들어진 것이 VPN, 즉 "가상 사설망"이다. 하지만 VPN은 **콘텐츠의 접속 우회 목적**으로도 사용할 수 있다.

예를 들어, 일본에 VPN 서버를 놓고, 한국에 있는 사용자 컴퓨터의 네트워크 트래픽을 전부 일본의 VPN을 거쳐 가도록 설정한다고 해 보자. 이렇게 하면 분명 사용자 컴퓨터는 한국에 있지만, 사용자 컴퓨터에서 나오는 트래픽은 우선 (인터넷상의) VPN 터널을 거쳐 일본에 있는 VPN 서버에 도착한 뒤, 그 VPN 서버에서 다시 나와 최종 목적지 서버로 향하게 된다. 그 결과, 실제로는 **한국에 있는 사용자가 접속한 것이지만, 목적지 서버가 볼 때에는 일본에 있는 컴퓨터가 접속한 것처럼 보**이게 된다.

게다가 일반적인 plain HTTP 프록시[4]와는 달리 사용자 컴퓨터와 VPN 서버 간의 연결은 암호화된다. 이 때문에 사용자가 거주하는 국가, 학교나 회사 등의 소속 단체, 혹은 통신사 등이 네트워크의 트래픽을 감청하거나 사이버 검열을 실시하는 경우에도, 최소한 사용자 컴퓨터로부터 VPN 서버까지의 구간에서는 암호화된 내용을 열어볼 수 없으므로 이를 회피할 수 있다. 다만, 대개의 경우 망을 감시하고 있는 국가, 학교, 회사, 통신사 등은 사용자가 VPN 서버에 접속했다는 것 자체는 알 수 있다[5].

VPN의 이러한 특성을 두고 많은 상용 VPN 사업자들이 '인터넷상에서 안전한 터널을 만들어 여러분의 정보를 지켜준다'는 식으로 광고를 하는데, 이는 반만 맞는 말이다. VPN의 암호화는 어디까지나 사용자 컴퓨터↔VPN 서버까지의 연결에 한하는 것이기 때문이다. 사용자 컴퓨터의 트래픽이 VPN 터널을 통해 VPN 서버에 도착한 뒤에는, VPN 서버에서 다시 나와 최종 목적지로 향하게 되는데, 이때에는 VPN의 암호화가 적용되지 않는다. 이 구간에서도 보안성을 유지하기 위해서는 SSL/TLS 등 별도의 암호화 기술이 필요하다.

주로 이 용도로 사용하기 위해, 세계 각국에 VPN 서버를 설치하고 요금을 낸 사용자에게 해당 VPN 서버에 연결해 인터넷을 사용할 수 있도록 해 주는 상용 VPN 서비스 제공자들이 있다. ExpressVPN, NordVPN, 미꾸라지 VPN처럼, 일반 사용자가 유료로 구매해 사용하는 이른바 "VPN"의 대부분은 이것을 가리킨다. 이 문서의 내용 중 대부분 역시 이러한 상용 VPN 서비스에 대해 서술한 것이다.

3.3. 적절한 서버 위치 선정으로 인한 인터넷 속도 향상

보통의 가정용 인터넷에서 보장하는 속도는 국내망에 한정해서이며, 해외망은 QoS나 각종 중계 등으로 인해 제대로 된 속도가 나오지 않는다. 그러나 데이터센터에 위치한 VPN 서버 같은 경우에는 해외망 또한 통신사가 속도와 지연속도를 보장하기 때문에 해당 문제에 민감한 사용자들은 VPN을 가입해 해외망 속도도 보장받을 수 있다. 특히 유럽이나 러시아 쪽으로 접속 시 보통 미국을 거쳐가거나 싱가포르로 접속 시 직통 회선이 없어 한참 헤매다 접속하기 때문에 속도가 느리지만 일본 데이터센터에 위치한 VPN은 직통으로 접속되기 때문에 체감이 크다.

4. VPN으로 오해하는 것들

4.1. 패킷 변조 애플리케이션

Intra, 유니콘 HTTPS, GoodbyeDPI 등은 단순히 https·SNI 검열을 우회해 주는 프로그램일 뿐, **기술적으로 VPN에 속하지 않는 것들이다.** 경찰의 추적이나 인터넷 검열을 피하는 도구로 알려져 있는데, 이런 것 중의 일부는 프록시 서버라고 불러야 한다. 심지어 저 중 일부는 프록시마저도 아니고 (자신의 IP를 변조하는) 우회로서의 기능도 없는 패킷 변조 프로그램이다. 시크릿 모드도 브라우저에만 기록을 남기지 않는 기능으로 VPN과는 무관하다.

VPN으로 착각하는 경우가 많은 이유는 활성화하면 기기에 VPN 프로파일이 추가된다는 점 때문인데, 이들은 **기술적**

으로 VPN이 아니다. 이들은 운영체제에서 제공하는 VPN 클라이언트 기능을 이용하여[6] 기기에서 발생하는 통신 패킷들을 받은 뒤, GoodbyeDpi처럼 변조 및 파편화(유니콘 HTTPS)(Intra 옵션)하거나, 그중 DNS 쿼리 패킷만 골라서 TLS로 암호화(Intra)할 뿐이다. 따라서 접속한 사이트 서버와의 통신 자체는 별도의 VPN 서버를 거치지 않으며, 사용자의 IP도 그대로 전달된다. **즉 사용자가 어느 사이트에 접속했는지 ISP가 알 수 있을 수 있으며[7], 목적지 서버[8]에는 사용자의 IP가 그대로 남아 있다.**

4.2. 프록시 서버

> VPN은 OSI 7계층에서 3번째 계층인 네트워크 레벨이고 프록시는 7계층(응용 프로그램) 입니다.
> 조금 쉽게 애기하면 3계층은 라우터가 하는 일입니다. 7계층은 우리가 쓰는 워드, 액셀, 게임 등등 입니다.
>
> 🔗 https://www.facebook.com/story.php/?story_fbid=858452949419699&id=100057650041660 🔗 @

VPN과 Proxy는 OSI 모형에서 계층이 다르다. VPN은 패킷의 터널링을 통해 가상 네트워크를 구축하는 데 목적이 있다면, 프록시는 특정 서비스(애플리케이션, 웹사이트)의 중계나 처리, 품질 향상에 목적이 있다.

IP우회의 관점에서 생각하면 VPN은 VPN 서버의 네트워크를 통째로 빌리는 것이라면, 프록시는 프록시 서버가 내가 접속하려는 사이트에 대신 접속하고 결과만 내 컴퓨터로 보내주는 방식이라고 생각해도 무방하다. 이러한 방법으로 둘 다 IP우회와 통신 암호화(VPN은 거의 필수적, 프록시는 선택적)가 가능하다.

프록시와 VPN 모두 IP 우회에 쓴다고는 하지만 우회에는 VPN이 보통 더 보편적이고 안전하다. 프록시는 애플리케이션 계층에서 처리하기 때문에 VPN보다 서버에 노출되는 정보가 더 많다. 때문에 IP 우회보다는 기업이나 웹서버에서 보안이나 로드밸런싱에[9] 쓰이는 경우가 훨씬 더 많다. 매우 거칠게 말하면 프록시는 애플리케이션 계층에서 정보를 중계하기 때문에 사용자의 애플리케이션(워드나 엑셀, 게임)에서 일어나는 일을 거의 다 알고 있어야 한다는 소리다. 반면 VPN은 네트워크 계층에서 정보를 중계하기 때문에 네트워크에서 일어나는 일들 예를 들면 정보가 어디서 와서 어디로 가는지 정도만 알아도 된다.

5. 보안성

5.1. 프로토콜상 익명성이 보호되는가?

🔗 VPN만 믿어서는 안되는 이유

VPN은 익명성을 위한 기술이 아니다. 어디까지나 단말기와 VPN 서버 사이의 통신을 암호화하여 터널링하는 기술일 뿐 익명성을 제공하지는 않는다. 만약 당신이 VPN을 쓰는 용도가 보안과 사생활 보호 때문이라면, Tor Browser를 쓰는 것이 훨씬 안전하다.

얼굴을 IP주소라고 할 때, VPN이라는 것은 가면을 쓰는 것이다. 얼굴이 보이지 않으니 완벽하다고 생각할 수 있지만, 가면을 파는 사람에게는 자신의 정보를 노출해야 하고 가면 그 자체에도 자신의 침이나 유전자가 묻어 나올 수가 있다. 반면 토르 브라우저는 가면을 파는 사람과 가면을 사는 사람 모두 각자를 알아볼 수 없게 철저하게 가리고 가면 내부를 코팅해서 가면을 쓴 사람의 유전자조차 남아 있지 않게 하는 것이다.

또한 사용자를 특정할 수 있는 것이 꼭 얼굴만 있지는 않다. 체형, 헤어스타일, 목소리, 옷, 신발 등 꼭 얼굴이 아니더라도 사용자를 특정할 수 있는 것은 상상 이상으로 많다. 가족과 친구는 가면을 쓰고 있다고 해서 지인을 못 알아보지 않는다. 만약 자신이 우회하기 전 IP로 로그인한 정보나, 저장된 쿠키나 세션정보를 브라우저에 남기고 있었다면 이를 토대로 추척할 수 있다. 또한 스마트폰이나 컴퓨터에서 백그라운드에서 동작하는 앱이나 서비스가 VPN의 IP로 자신의 계정 정보를 지속적으로 전송하고 흔적을 남길 수 있다. 토르 브라우저가 항상 별개의 브라우저로만 실행되는 이유는 이러한 정보의 노출을 최소한으로 줄이기 위해서이다.

VPN이 노 로그라도 VPN서버의 데이터센터는 로그를 남길 수 있기 때문에 VPN으로 정말 위험한 행동은 하면 안 된다.

VPN이라는 이름, 즉 '가상 사설망'이라는 이름 자체만 보더라도 이 기술이 익명성과 프라이버시 보존 목적이 아니라는 것을 볼 수 있다. 본 문서 개요에서 보듯 '사내망을 가상으로 구성하여 외부에서 접근하는 등의 목적'에서는 오히려 개개인이 더 잘 식별되어야 할 필요성이 있다. 외부인이 사내망에 불법으로 접근하여 기밀을 유출하거나 할 수 있는 상황을 가정하면 '익명성' 따위를 VPN 기술에 집어넣는다는 것은 사실상 자살행위나 마찬가지다.

VPN 회사들이 체험판 VPN에 접속한 로그를 기록해 두었다가 광고업체나 수사기관에 가져다 바친다는 내용은 부분적으로 사실이다. 이는 VPN 유료 서비스를 이용하더라도 해당될 수 있다. VPN을 홍보하는 광고 목적의 사이트를 보면 파이브 아이즈 및 파이브 아이즈 국가와 협력하는 포틴 아이즈 / 기타 협력 국가들의 사용자 정보 수집 및 국가기관에의 제공 여부를 우려하고 있으며 이 국가들 밖에 본사를 둔 VPN 따위를 안전하다며 홍보하는 글을 쉽게 찾아볼 수 있다. 이는 프리즘 폭로 사건 때 미국뿐만 아니라 타국에서의 이용자 데이터 수집 행위 논란 이후로 불거진 것으로, 실제로 미국의 PureVPN은 **FBI에 정보를 넘겨주었다가 신뢰도가 급락하여** 엄청난 이용자 감소가 있었다. 또한 VPN 제공 업체가 '파이브 아이즈' 및 미국과 사이버 정보를 공유하고 있지 않는 곳에 본사를 두고 있지 않더라도 그들이 사용하는 **VPN 서버** 자체는 대부분 타국에 있다는 것을 알아야 한다. 웬만큼 잘 나간다는 VPN 업체들은 미국, 일본, 영국 등을 포함해 수많은 나라에 서버를 두고 있다. 그래서 VPN 사용자를 추적하는 법에는 해당 VPN 제공 업체에 로그를 내놓으라고 하는 것이 아니라, 그들이 사용하는 VPN 서버에 접근해서 기록을 얻어내는 법이 있다. 또는, 해당 VPN 서버는 결국 현지의 ISP와 통신하면서 인터넷을 제공해야 하는데, 해당 ISP에서의 접속 기록을 추적하여 이용자를 탐색하는 법이 있다. 실제로 2014년 네덜란드 경찰은 absolutely no logs라고 광고하는 VPN 회사인 EarthVPN 유저를 검거하기 위해 EarthVPN 회사는 아예 건너뛰고, 해당 VPN의 서버가 위치해 있는 데이터센터 로그기록을 입수하여 EarthVPN 유저를 검거했다. 🔗# 이러한 사실을 VPN 홍보글에서는 절대 언급하지 않는다. 또한 많은 VPN사이트의 약관에는 광고 목적으로 사용자 접속 정보를 이용할 수 있도록 하는 조항이 추가되어 있는 경우가 매우 많다. 또한 약관에 표기되어 있지 않더라도 몰래 사용자 정보를 수집하는 것으로 의심되는 업체의 사례도 있다.

Tor 네트워크는 악성노드들이 데이터를 가로챌 위험이 높아 VPN을 써야 한다는 VPN 제휴 사이트의 홍보글을 볼 수 있다. 하지만 어니언 라우터 기법을 사용하는 Tor도 특성상 각 노드들이 얻을 수 있는 정보는 매우 제한적이다. 오히려 VPN이 더 위험한데 VPN 서버를 운영하는 기업이 모든 트래픽을 들여다 볼 수 있기 때문에 실제로 상당수의 무료 VPN들은 이를 활용해 사용자의 개인 정보를 수집해서 팔아먹고 일부 극단적인 VPN은 계정 정보까지 탈취하기도 한다.

VPN 서버에 대한 가장 큰 오해는 VPN을 운영하는 기업이 전 세계에 개별적인 서버를 소유하고 있다고 착각하는 것이다. 하지만 대부분의 VPN 서버는 AWS같은 IaaS 데이터 센터의 서버 일부를 임차한 뒤 VPN 서버로 구성을 한다.

VPN을 사용함으로써 얻을 수 있는 유일한 익명성은 실제 단말기의 IP 주소를 숨긴다는 것 말고는 없다. 또한 적절히 IP가 숨겨졌다고 가정해도 하드웨어[10] 정보, 쿠키, 브라우저 핑거프린팅, 계정정보 같은 다른 식별정보는 전혀 숨겨지지 않는다. 🔗IP를 우회했지만 구글 메일을 사용해 꼬리가 잡힌 일베 유저 또한 서비스 업체가 사용자가 VPN을 사용한다는 사실 자체는 **아주 쉽게 알아낼 수 있다.** 그냥 어떤 VPN 서비스를 결제해 보기만 해도 알 수 있기 때문이다. 무료든 유료든 VPN을 가동하고 자신의 현재 IP를 표시하는 사이트 등에 들어가면 VPN 대역 IP는 금방 알 수 있다. 애초에 VPN 클라이언트 자체에서 자랑스러운 듯 '현재 위치를 확인해 보세요! 당신의 정체가 잘 숨겨졌습니다!' 라고 이런 사이트들로 향하는 버튼을 만들어두기도 한다. 현재 넷플릭스만 하더라도 🔗VPN이 감지되면 차단 하고 있으며, 나무위키 또한 대부분의 VPN을 차단하기 때문에 VPN을 켜고 들어온다면 편집이 불가능하다. VPN 업체들은 이런 차단 자체를 근본적으로 무력화할 수 없다. 기껏해야 주기적으로 다른 서버를 확보해 다른 IP를 제공하는 것뿐이다. 그리고 브라우저 핑거프린팅, 유저 에이전트 등을 사용하면 VPN을 사용하더라도 개개인을 은폐할 수 없다.

다음과 같은 상황을 가정하자. 유튜브에서 지역락이 걸린 영상을 시청하기 위해 이미 한국 IP로 매일같이 접속하던 계정에 로그인한 상태로 VPN을 사용한다면, 사용자의 credentials, 즉 사용자 계정 자체에 로그인하기 위해 사용되는 세션은 그대로이며[11] 전혀 은폐되지 못한다. 구글 서버의 계정 기록에는 늘 한국에서 접속하던 계정이 갑자기 제3국 I

P로 접근한다면 당연히 VPN 사용으로 의심될 것이다. 설령 VPN용 계정을 새로 파고 이 계정을 사용할 때는 항상 VPN을 사용한다 하더라도, 기기 ID 정보를 통해 예전에 한국 IP만 사용하던 기기가 갑자기 외국에 있는 것으로 나타나며, 조금 뒤에는 그 기기에서 다른 계정이 한국 IP로 접속한 게 나타난다면 당연히 구글에서는 이를 모를 리가 없다. 아예 기계까지 새로 구하면 조금은 까다로워질지도 모르지만 고작 유튜브 지역락을 우회하고 이를 숨기기 위한 목적으로 벌써 수십만 원 이상의 돈이 나갔다. 이렇게까지 할 유저가 있을지는 의문이다.

막장 업체도 의외로 많아서 신용장사 할 듯이 잠깐 띄우고는 돈은 돈대로 먹튀하고 그동안 뽑아낸 정보는 정보대로 팔아치우는 경우가 없다고도 할 수 없다. 그러므로 유료 VPN이라고 무조건 믿어서는 안 되며, 사용할 것이라면 믿을 만한 보안업체에서 제공하는 VPN을 사용하는 것이 좋다.[12]

요약하자면 유료 VPN을 사용하는 것은 **자기 자신을 숨기고 익명화하기 위함**이 아니라 **단순히 외국 IP를 사용하는 것 자체**에 두는 것이 타당하다. VPN을 홍보하는 수많은 광고성 글에서도 '넷플릭스 보기 좋은 VPN' 따위의 글들을 추천하고 있다. VPN을 사용하면 VPN 서버가 사용자와 목표하는 인터넷 서비스 사이의 모든 통신 내역을 볼 수 있으며, 아무리 '로그 저장 없음' 따위를 광고한다 할지라도 **이를 신뢰할 수 없으니** 당신의 VPN 사용 내역은 모두 기록될 수 있으며 이미 기록되고 있다고 가정해야 한다. 따라서 애초에 '공개되더라도 그렇게 부끄럽지 않고 떳떳한' 활동이나 하는 것이 낫다. 대부분의 경우 VPN을 사용하는 것은 지역락이 걸린 콘텐츠를 우회하여 이용하거나(유튜브, 넷플릭스 등) 온라인 게임의 외국 서버를 이용하며 렉을 조금이라도 감소시키기 위한 것, 한국의 경우에는 warning.or.kr을 우회하는 것 등이 있다. 대한민국의 경우 포르노의 제작 및 배포가 불법일 뿐 시청이 불법이 아니며 차단 조치를 우회하는 것 또한 불법이 아니다. 일부 악플러 등이 VPN을 사용했기 때문에 잡히지 않는다는 것 때문에 VPN이 익명성 제공 툴로 오해받는 경우가 있으나, 이는 VPN 프로그램 제작국 또는 서버 소재지 등(대부분 미국이나 유럽 선진국)에서 사실적시 명예훼손을 범죄로 여기지 않으며, 수사력의 한계로 인해 용의자의 IP가 해외로 나오면 수사를 중단하는 관행 때문일 뿐이다.[13][14]

많은 유저들이 사용하는 츠쿠바 대학교 대학원의 무료 VPN인 VPN Gate같은 경우에는 **범죄행위 방지를 위해 모든 접속로그가 자동으로 기록되고 있다.** 라는 경고문이 포함되어 있다. 이는 특수한 경우로 VPN Gate는 애초에 상업적이 아닌 학술적 목적으로 운영되는 VPN 서비스이기 때문. 범죄에 악용된다는 비난을 피하기 위해 악용할 경우 대응하기 위해 게이트웨이 접속 로그를 백업해두겠다는 의미로 해석된다.

어떤 정보를 수집 저장하는지 문의해 본 결과 백업하는 항목은 OS Ver, Web Browser Name, MacAdress, IP(User,rent,root,isp name), Time stamp, Traffic Used이다. 이 6가지 정보를 수집 및 기록하고 있으며 12개월(User IP가 유럽인 경우 한정 6개월)간 저장한다. 위 정보는 국가를 가리지 않고 수사 기관이 일본 또는 미국의 법률에 근거해 합법적인 요청이 있을 경우 제공되고 있으며, 해당 기록을 토대로 사이버 범죄자를 체포하는 데 많은 공헌을 했다고 하며 FBI나 ICPO와는 항시 협조중이라고 한다.[15]

5.2. 해킹이 불가능한가?

당연히 가능하다. 실제로 VPN 프로토콜이 구형이거나 업데이트가 되어 있지 않거나, 암호나 인증서를 노출하거나 약하게 설정한다면 스크립트 키디 수준의 해킹에도 무방비로 노출될 수 있다. 신형 프로토콜도 취약점이 존재할 수밖에 없기 때문에 해킹이 불가능한 건 아니다. 가격이 비싸서 정보기관 등에서만 사용할 뿐이다.

미국의 NSA는 VPN 암호코드를 해독하는 데 성공해 **이를 패킷단위로 실시간 감시하는 모습을 보여주기도 했다.**[16] NSA라도 무식하게 암호화를 해독하는 방식은 사실상 불가능하고, 아마 VPN 프로토콜의 취약점을 이용하거나 VPN 서버나 소프트웨어에 백도어를 심어놓는 등의 방법으로 공격하고 있을 것이다. 아무리 AES-128 암호화라도 현대의 컴퓨터 기술로는 유효한 시간 내에 해독하는 것이 사실상 불가능하다.

위의 뉴스 기사는 2013년도이고, 자세한 내용이 나와 있지 않으며 반대 의견도 있다. AES-256bit 암호화를 해독하려면 고성능 컴퓨터를 몇십 년 굴려도 어려운 수준이다. 또한 취약점을 이용한다고 하더라도 일부 VPN 서버에 로그가 남을 수밖에 없고 이걸로 전 세계의 VPN을 모니터링한다면 당연히 발각될 위험이 커지기 때문에 실시간으로 전 세계의 암호화 트래픽을 모두 해독한다는 것은 사실상 불가능한 일이라는 것.

2026년 5월 23일 유로폴은 범죄자 VPN 네트워크 1vpns.org를 차단하고 도메인을 압수했다. vpns.org는 2014년부터 시작하여 적어도 25개의 랜섬웨어 그룹이 범죄에 사용했고 해킹 등 여러 사이버 범죄에도 사용되었다. 1vpns는 로그를 저장하지 않아 법의 추적을 피할 수 있는 신뢰할 수 있는 범죄 네트워크로 홍보해왔으며 익명 결제 및 범죄 행위에 특화된 VPN서비스를 제공해왔다. 18개국 수사기관의 국제 합동 작전으로 2021년 12월 조사가 시작되어 해킹을 통해 서버의 위치를 파악하고 우크라이나 소재의 운영자 체포 및 33대의 서버를 압수하여 일망타진했다. VPN서버에 남겨진 로그를 통해 83건의 진행 사건 및 506명의 용의자를 파악하여 추가 수사 중이다. 유로폴은 1vpns사용자에게 서비스 중단 및 이용자의 신원을 확인했다는 사실을 통보했다.

5.3. 이용자 로그 제공?

무료 VPN이라면 이용자의 로그를 쉽게 받을 수 있지만 유료 VPN은 얘기가 다르다.

이론적으로는 유료 VPN 회사가 고객의 개인정보를 제공한다면 이용자를 특정할 수 있다. 그러나 현실적인 문제 네 가지가 있다.

1. 유료 VPN 회사의 입장에서는 제3자에게 고객의 개인 정보를 제공하면 고객의 신뢰를 잃을 수도 있기 때문에 중대한 사유가 아니라면 제3자에게 고객의 개인정보를 제공해 주지 않는다.

2. 유료 VPN의 서버를 전원을 끄면 정보가 날아가는 RAM으로 운영하는 경우도 많다. 이 경우 제공해 줄 로그 자체가 사라져서 없다.

3. 유료 VPN 회사에서 자료를 제공해 준다고 해도 방대한 자료 속에서 찾고자 하는 자료를 찾는 것은 어렵다. 네트워크 상에서 생기는 수많은 패킷 속에서 유저를 찾아내는 것은 힘들다. 사막에서 바늘을 찾는다고 생각하면 된다.

4. 수사기관의 수사력과 행정적 비용은 무한대가 아니다. 수사기관이 맡고 있는 사건은 많으므로 하나의 사건에 한정된 자원을 모두 쏟아부을 수는 없다.

국내 기업의 VPN은 법적으로 이용자 로그 저장 및 정보 제공이 강제되므로 프라이버시가 목적이라면 무조건 걸러야 한다. #

유료 VPN의 한국 IP를 이용할 때 해당 VPN 한국 IP의 서버가 실제로 한국에 있는 물리 서버인지, VPN IP는 한국으로 뜨지만 서버는 해외에 있는 가상 서버인지 확인해야 한다. 만약 물리 서버라면 한국의 법 때문에 로그를 강제로 남겨야 하므로 절대 쓰면 안 된다. **무조건 가상 서버만 이용해야 한다.** #

비록 토어 네트워크가 제공하는 익명성보다는 약하지만 속도는 유료 VPN이 훨씬 더 빠르다.

인터넷상에서 정말 중대한 범죄를 저질렀다면 유료 VPN을 썼더라도 특정될 수 있으니 범죄를 저지르지 않는 것을 권한다. 만약 잡히지 않더라도 애초에 범죄는 도덕적으로 옳지 않은 행동이다.

6. VPN 구축 및 이용

6.1. 사설망(인트라넷) 구축 목적

6.1.1. VPN 장비

아마존닷컴에 있는 VPN 클라이언트 기능을 지원하는 라우터.

VPN 장비는 VPN 서버 또는 클라이언트 기능을 하는 독립된 장비이다.

VPN 서버나 클라이언트를 지원하는 공유기는 생각보다 많다. L2TP는 웬만해서는 다 지원하고, 조금만 돈을 더 쓰면 OpenVPN을 지원하는 물건까지 나온다. 다만 공유기 네트워크 칩셋 자체의 연산성능이 그리 좋지는 않기 때문에 속도는 AC88U 같은 상급 공유기로 잘 뽑아줘야 30~35 Mbps 정도로 크게 기대하지 않는 것이 좋다.

한국 내에서 가장 흔하게 쓰이는 아이피타임 공유기의 경우, 꽤 오랫동안 VPN 서버만 지원하고 클라이언트 기능을 지원하지 않았다가, 2022년 3월, 드디어! 지원이 발표되었다. 모든 제품이 다 지원하는 것은 아니고, 28종의 제품만 된다고 한다.# 아예 대놓고 무료로 .ovpn 파일을 받을 수 있는 VPN Gate 주소를 안내하는 건 덤.[17]

24시간 내내 안정적으로 빠른 속도를 원한다면 데스크톱 또는 노트북에서 주로 쓰는 x86_64 CPU를 사용하는 컴퓨터에 듀얼랜 이상 랜카드 박고 라우팅 전용 OS를 올린 공유기를 직접 만들어야 한다. 일명 **소프트웨어 라우터**라고 불리기도 한다.

이런 VPN은 보통 사설망 구축 목적으로 사용하지만 유/무료 VPN 회사에서 공유기가 지원하는 프로토콜을 지원한다면 IP 우회 목적으로도 사용이 가능하다.

6.1.2. VPN 서비스

Hamachi, Tailscale 등 컴퓨터에 설치해서 쉽게 사설망을 만들 수 있는 VPN 소프트웨어가 있다.

중앙서버를 제공하는 곳도 있지만 주로 장비끼리 직접 연결하는 메쉬 VPN이 쓰인다. 직접 연결이 어려운 내부망에서 접속하기 위해 중앙서버와 메쉬의 하이브리드 형태로 된 경우도 많다.

6.2. IP 우회 목적

IP 우회 목적으로 VPN을 쓴다면 주로 직접 구축하기보단 외국 업체의 IP 우회용 유료 VPN 서비스를 이용할 것이다. 인터넷에 널려있는 각종 VPN 리뷰는 되도록이면 거르자. 과반수가 VPN 업체와 제휴를 맺고 뒷광고를 하는 곳이다. 고객이 그 리뷰 사이트의 링크를 타고 VPN 회사 홈페이지로 넘어가서 유료 VPN을 결제하면, 1개월 결제 시 결제금액의 100%, 6개월~1년 결제 시 결제금액의 30~40% 정도를 VPN 업체가 리뷰어에게 준다. 흔히 해외 유튜버들이 자주 맡는 스폰서 광고와 결과적으로 똑같지만 광고가 아닌 척 하는 경우다.

또한 VPN을 리뷰하는 사람들은 대체로 NordVPN과 ExpressVPN을 추천한다. **이 두 업체에서 리뷰 수수료를 가장 많이 쳐주기 때문이다.** 물론 (보안 수준은 좀 다른 문제지만) 회사 홍보비와 클라이언트 소프트웨어의 편의성은 어느 정도는 정비례하는 경향은 있다. 장기간에 걸쳐 거액의 홍보비를 뿌릴 정도의 재정이 있다면 적어도 고객 눈에 보이는 부분의 품질 향상에 투자할 수 있는 자금 여력도 있기 때문이다. 많은 홍보비를 집행하지만 실제 유저들에게는 파도 파도 괴담만 나온다는 수준의 평가를 받는 서비스가 아니라면 대체로 서비스의 기본은 충족하고 소비자에게 사기를 치는 행위는 잘 일어나지 않는다고 보면 크게 틀리지는 않는다. 클라이언트 프로그램 퀄리티나 접속 안정성 등 기본적인 기능들이 용납이 안 되는 수준이라면 리뷰 수수료를 얹어줘도 이런 제품이 소비자들에게 장기적으로 보통 이상의 평가를 받기는 힘들다. 한때 맥 유저 타겟 인터넷 광고를 거의 독식해 버리다시피 했던 MacKeeper 같은 소프트웨어도 거액의 홍보비를 집행했지만 맨틀에 쳐박힌 수준을 넘어 내핵으로 향하는 최악의 사용자 만족도를 개선한 적이 없었고 오히려 애플 유저의 저주와 증오를 독식하는 독보적인 수준의 악평을 구축한 전적이 있다. 그렇기 때문에 홍보비만으로 인터넷 여론 전체를 매수할 수 있다는 가정에는 좀 무리수가 있다고 볼 수 있다.

어떤 VPN이 보안을 신경 쓰고 성능이 좋은지는 본인이 직접 판단하여 고르는 게 좋다. 정 찜찜하면 AWS나 Azure의 국외 reigon에 위치한 적당한 성능의 인스턴스를 하나 임대해서 직접 개인용으로 구축하는 것도 고려해 볼 만하다. 예산만 된다면 안정성은 확실해지는 셈이니까.[18]

6.2.1. 무료 VPN

VPN은 공개서버가 많은 프록시 서버와 달리 기본적으로 사설망 형식으로 운영되므로 구축과 운영에 반드시 비용이 발생한다. SoftEther VPN 같은 학술, 연구목적 같이 별도 지원을 받지 않는다면, 자원봉사가 아닌 이상 다른 방법으로 수익을 창출해야만 한다.

세상에 공짜는 없다. 무료 VPN은 사용자의 개인정보를 팔아넘기고, 리소스를 활용하여 수익을 창출한다. 참조 당신의 개인정보를 지키고 싶다면 무료 VPN은 아예 쳐다보지도 말아야 한다. 상식적으로 무료 VPN 업체들이 자원봉사자도 아니고, 전 세계 유저들에게 아무런 대가 없이 서비스를 제공하진 않는다. 유료 VPN과는 달리, 무료 VPN업체들은 서비스에 수익이 없기 때문에, 몰래 FBI등 수사기관과 협조하여 개인정보를 수사기관에 넘기는 일마저 발생하였다.

네이버와 다음 같은 곳에서 검색하면 나오는 무료 VPN은 앞서 적힌 내용과 같이 일부 트롤들의 도구로 사용되어 몇몇 국내 사이트에는 접근이 불가능한 경우가 있으며, 속도는 사실상 포기해야 마음 편해진다. 특히 가장 유명한 무료 VPN인 SoftEther VPN은 대한민국 유저 3,200만 명이 **무려 12페타[19]를 쓰며 1위를 찍는다.** 2위인 중국은 3억 392만 명이 5.3페타를 쓰니 엄청난 차이.[20] 그렇기 때문에 무료 VPN은 잠깐 동안 IP 우회의 용도로만 쓰는 것을 추천한다.

무료 VPN의 속도가 마음에 안 들지만 그렇다고 유료버전을 사용하기 부담스러운 유저라면 트라이얼 버전을 사용하는 방법도 있다. 다만 일정 기간 동안 상용기능을 체험하는 트라이얼 버전은 사용 조건이 대개 **신용카드 정보 사전 등록**이기 때문에 트라이얼 종료기간을 잊으면 자동결제가 되어 카드에서 나가는 돈을 보고 눈물 쏟는 경우도 있다.

대개는 달팽이 저리 가라 할 속도를 자랑하지만 그나마 무료 상태에서도 안정적인 속도를 내주는 곳이 있다. 이런 곳은 회선에 간섭해서 광고를 띄우는 편이다. 즉 브라우저에서 원래 떴어야 할 다른 광고의 호스트에 자사 광고 콘텐츠 주소로 매핑해 버려서 자사 광고를 끼워넣는 곳이다.

본인이 구축하면 VPN 자체는 무료 VPN인 것이다. 아래 구축용 소프트웨어 문단으로. 이게 뭔 의미가 있을까 싶을 수 있지만 밖에서 통피가 아닌 집피를 쓰고자 할 때 쓸 수 있는 수단 중 하나가 될 수 있다.

6.2.2. 유료 VPN

윈도우에서 안전하게 익명으로 인터넷 하는 방법

PrivacyGuides 권장 VPN

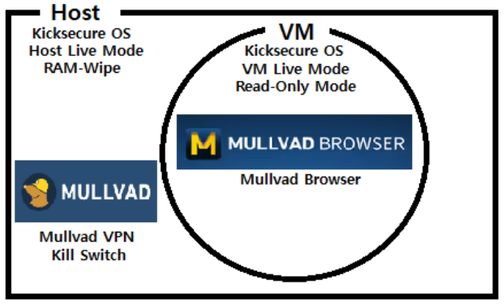
+

Mullvad 브라우저

OR

Tor 브라우저

리눅스에서 VPN으로 안전하게 인터넷 하는 방법



Kicksecure OS: 보안이 강화된 데비안 기반 OS
Live Mode: 종료 시 초기화 됨.
RAM-Wipe: 종료 시 RAM에 있던 내용이 삭제 됨.
Read-Only Mode: 읽기 전용 모드.
Kill Switch: VPN이 꺼지면 인터넷이 끊기도록 함.
Mullvad VPN & Mullvad Browser: 프라이버시를 위한 VPN과 브라우저.
* 만약 Virtualbox를 사용한다면, 가상 디스크 이미지 모드를 설정할 때 먼저 가상 디스크를 분리한 다음에 Immutable 모드 또는 Normal 모드로 설정해야 함.
* Tails OS의 안티포렌식은 좋은데 Tor 네트워크가 너무 느려서 답답한 사람들을 위한 방법임.

참고 링크
https://www.kicksecure.com/wiki/About
https://www.kicksecure.com/wiki/ISO
https://www.kicksecure.com/wiki/VirtualBox
https://www.kicksecure.com/wiki/KVM
https://www.kicksecure.com/wiki/Live_Mode
https://www.kicksecure.com/wiki/Ram-wipe
https://www.kicksecure.com/wiki/Read-only
https://www.virtualbox.org/manual/topics/storage.html
https://www.privacyguides.org/en/vpn/
https://www.privacyguides.org/en/desktop-browsers/

VPN 관련 글

2022년 2월 6일, 🔗 각 VPN의 장점과 단점 그리고 리뷰[21][22][23]
2023년 3월 7일, 🔗 프라이버시 VPN 추천

2020년 8월 ~, 🔗 Privacy Guides의 추천 VPN 🔗 @: Mullvad VPN, IVPN, Proton VPN은 보안 커뮤니티에서 삼신기, 삼대장으로 불리며, PrivacyGuides에 정식으로 등재되어 있는 대표적인 VPN 서비스이다. 이 VPN들은 이용자들의 개인정보 보호를 진지하게 여기기로 알려져 있다. 🔗 참고
2021년 4월 15일, 🔗 VPN 마케팅의 문제점
2021년 6월 2일, 🔗 오픈소스가 좋은 이유
2021년 6월 3일, 🔗 Exoressvpn의 제휴 마케팅(11번 항목)
2021년 6월 21일, 🔗 판다 VPN, 킹콩 VPN 비판, 🔗 #
2021년 7월 22일, 🔗 NordVPN 비판(6번 항목), 🔗 #
2021년 9월 19일, 🔗 VPN별 트래커 개수[24]
2021년 10월 8일, 🔗 ExpressVPN 회사의 신뢰성 논란, 🔗 #
2022년 3월 ~, 🔗 제휴 마케팅에 대한 Mullvad 회사의 입장 🔗 @[25]
2022년 3월 6일, 🔗 NordVPN, Surfshark 회사의 신뢰성 논란
2022년 3월 8일, 🔗 VPN 트래커 관련 글
2022년 3월 8일, 🔗 한국회사 VPN은 무조건 걸러야 하는 이유
2023년 2월 17일, 🔗 VPN 한국서버를 조심해야 하는 이유
2022년 3월 28일, 🔗 VPN회사 신뢰성 논란 관련 글
2022년 4월 27일, 🔗 삼신기가 추천받는 이유
2022년 7월 3일, 🔗 Mullvad의 여러 장점
2022년 10월 3일, 🔗 VPN들의 보안은 대부분 동일함: 프라이버시 관련 커뮤니티에서 보안이 좋은 VPN을 추천해달라는 질문이 자주 나온다. 그러나 보안과 프라이버시는 다른 개념이고 정말 쓰레기 VPN이 아닌 이상 대다수 VPN들은 보안이 동일하다.

VPN 속도 비교

2021년 9월 21일, 🔗 비교글1
2022년 3월 22일, 🔗 비교글2

○, ◎: 있음 / △: 부분적으로 있음 / ×: 없음

서비스	소재지	로깅					비트코인 결제	모네로 결제
		트래픽	DNS요청	타임스탬프	대역폭	IP주소		
ADGUARD VPN	키프로스	×	×	×	△(1)	×	지원	미지원
ExpressVPN	영국령 버진아일랜드	×	△(2)	○	○	×	지원	미지원
Hotspot Shield	미국	○	○	○	○	○	미지원	미지원
IVPN	영국령 지브롤터	×	×	×	×	×	지원	지원
MULLVAD VPN	스웨덴	×	×	×	×	×	지원	지원
NordVPN	파나마	×	×	×	×	×	지원	미지원
ProtonVPN	스위스	×	×	×	×	×	지원	미지원
SoftEther VPN	일본	○	○	○	○	○	무료 소프트웨어	
Surfshark	네덜란드	×	×	×	×	○(3)	지원	미지원
windscribe	캐나다	×	×	×	×	×	지원	지원(4)

(1) 무료 버전 사용자에 한하여 ○
(2) 인터넷 감시 재단(IWF) 과 협력해 아동 성착취물(CSAM) 관련 정보가 있는지 검사하고, 발견되면 차단함. 로깅은 하지 않음
(3) 부정행위(무제한 접속 악용) 방지를 위해 연결 시 사용자의 IP 주소를 일시적으로 암호화된 형태로 저장하지만, VPN 연결 종료(세션 종료) 15분 후 자동 삭제된다.
(4) 프로 플랜 및 일부 결제 수단에 한하여 지원

애초에 대한민국에서 VPN을 서비스 하는 업체들은 대부분 기업들을 대상으로 하기 때문에 가격 개념 자체가 다르며, 무엇보다 제공하는 IP가 대부분 국내(대한민국) IP이다.[26] 개인을 대상으로 세계 각국의 IP를 제공해 주는 업체들은 대부분 해외업체들이다. 결제수단은 신용카드 혹은 페이팔이다. 익명성을 중시한다는 점 때문에 비트코인 결제를 받는 곳도 있다. 비자나 마스타카드를 지원하는 체크카드도 받기 때문에 학생들도 어느 정도 기본적인 영어실력만 있다면 크게 무리 없이 결제가 가능하다. 다만 거의 대부분의 업체가 **매달 자동결제로 등록된다.** 추후 사용계획이 없다면 반드시 해약하자.

유료로 VPN을 서비스하는 기업은 영어로 검색하면 생각보다 간단하게 찾을 수 있다. 가격대는 매달 5달러부터 20달러까지 다양한 편이지만, **같은 가격임에도** 서버 퀄리티가 심하게 차이난다. 같은 돈 10달러 내면서 서버 한대에 속도마저 시망인 곳이 있다면, VPN 서버가 몇십개이면서 속도도 빵빵한 곳도 있다. 그렇기 때문에 반드시 트라이얼 버전을 통해 최종구매 전에 테스트해 봐야 한다.

하지만 한국인의 유료 VPN 사용률이 높아짐에 따라, VPN 시장에서 한국인 고객들이 많아지고 있다. 이런 한국인 소비자들을 잡기 위해 결제도 대한민국 원으로 할 수 있게 바꾸고, 깔끔하게 번역된 한국어 홈페이지와 설명서를 지원하는 해외 VPN 업체도 생기고 있다. 다만 대한민국 원으로 결제를 받는 곳들 중에는 DCC를 통해 환전 수수료 폭탄을 선사하는 곳도 있기 때문에 주의해야 한다. 2020년대 초 들어서는 한국 신용카드를 직접 받는 곳도 늘어나고 있다.

생각보다 사기가 많다. 유료 VPN인데 서버가 부실해서 지정한 국가와 다른 서버와 연결되기도 하고 결제하면 평생 무료 같은 말로 소비자들을 속이기도 한다. 특히나 페이팔과 같은 에스크로 결제 서비스를 거치지 않고, 신용카드 정보를 직접 입력하는 결제만 가능할 경우 강하게 의심해야 한다. 페이팔같은 에스크로 서비스는 설사 사기라 해도 자동결제를 바로 해약하여 추가피해를 막을 수 있지만, 신용카드 정보를 직접 제공해 주면 무승인 거래에 걸려 재수없으면 영원히 해약이 불가능한 상황에 빠질 수도 있다. 무승인 거래는 한번 승인되면 **카드를 없애버려도 가맹점에서 청구를 할 수 있다.** 무승인 결제는 한번만 승인나면 잔고없는 체크카드라도 결제가 되기 때문에 의심되면 절대 카드정보를 제공해선 안된다.

1회 결제로 평생 사용이 가능하다는 VPN의 경우 중간에 연장 신청을 하지 않으면 계정이 막히는 곳도 있고, 대부분 성능이 좋지 못한 경우가 많으며 서버 유지 비용도 나오지 않는 돈을 받고 운영하는 데에 있어 정보 판매가 이루어지지 않느냐는 의혹도 있다.

참고로 위의 Surfshark, NordVPN, ExpressVPN 등[27]은 Shopback, RebatesMe 등의 캐시백 사이트를 통해 돌아가며 주기적으로 행사를 하는데 장기구독권을 100% 캐시백해 줄 때도 있다.[28] 딱히 높은 프라이버시 보호가 필요한 것은 아니지만 유료VPN이 필요하다면 노려보자.

6.2.3. 웹서핑 시 프라이버시 지키기

유료 VPN을 쓰고 있으니 이제 나의 프라이버시가 지켜지고 있다고 착각하는 사람이 많다. 그러나 프라이버시를 지키려면 생각보다 많은 것을 알아야 한다. 관련 정보를 얻기 위해 이 문서와 Tor, 인터넷 프라이버시 문서를 둘 다 참고할 수 있다. 예를 들어서, 유료 VPN을 쓴다 해도 크롬을 사용한다면 프라이버시가 전혀 보호되지 않는다.🔗 관련글

2022년 6월 28일, 🔗 시크릿 모드는 만능이 아니다
2021년 10월 13일, 🔗 어플보다는 브라우저를 쓰는게 더 좋은 이유,🔗 #
2022년~, 🔗 Privacy Guides의 추천 PC 브라우저🔗 @[29]
2022년~, 🔗 Privacy Guides의 추천 모바일 브라우저🔗 @[30]
2023년 5월 4일, 🔗 Arkenfox로 파이어폭스 강화하는법[31]
2022년 4월 ~, 🔗 Privacy Guides의 추천 검색엔진🔗 @[32]
2023년 2월 6일, 🔗 안드로이드 킬스위치 설정[33][34]
2021년 12월 18일, 🔗 좋은 비밀번호를 만드는 방법,🔗 #,🔗 #[35][36]
2023년 3월 7일, 🔗 무료 클라우드 서비스 추천
2022년 8월~, 🔗 Privacy Guides의 추천 메신저🔗 @[37]
2022년 4월~, 🔗 이미지 메타데이터 삭제 프로그램🔗 @[38][39]
2023년 10월 6일, 🔗 안전하게 PDF 읽는 방법,🔗 #[40][41]
2021년 9월 28일, 🔗 DNS 유출 방지법🔗 @
2022년 3월 10일, 🔗 WebRTC 유출 방지법🔗 @

6.2.4. 토렌트 사용 시 프라이버시 지키기

유료 VPN 쓰고 있으니 마음껏 토렌트를 써도 안전하다고 착각하는 사람이 많다. 그러나 적절한 조치를 하지 않으면 프라이버시가 보호되지 않는 것은 물론 자신의 신원이 드러나 곤란한 상황에 빠질 수 있다. 참고로 VPN이 다운받은 파일에 심어진 악성코드를 없애지는 못하니 백신이나 가상머신을 이용한다.

무료 VPN이나 값싼 VPN의 경우 BitTorrent 기능을 지원하지 않아 업로드와 다운로드가 정상적으로 진행되지 않는 경우가 많다.[42] 이름 있는 유료 VPN의 경우에도 일반 서버의 경우 토렌트를 막아놓은 경우가 많으니 P2P 전용 서버를 활용하자.

또 어떤 VPN들은 SOCKS5 프록시를 지원하는데, 여러 토렌트 클라이언트 역시 프록시를 지원하므로 이를 통해 킬스위치를 만들 수 있다.

2021년 1월 12일, 🔗 VPN으로 토렌트 돌릴 때 꼭 읽어야 하는 글,🔗 #
2023년 3월 8일, 🔗 qbittorrent 설정 가이드,🔗 #
2022년 3월 9일, 🔗 qBittorrent가 좋은 이유,🔗 #
2019년 2월 19일, 🔗 킬스위치가 필수인 이유
2022년 5월 21일, 🔗 P2P 핑거프린팅🔗 #🔗 #[43][44]
2022년 8월 10일, 🔗 토렌트 설정 관련글 🔗 @

7. 다양한 분야에서의 활용

가상 사설망은 인터넷 검색 등의 일반적인 용도 이외에도 다른 목적으로도 이용되기도 한다.

7.1. 오락실에서의 이용

본래 오락실에서는 이러한 네트워크를 쓸 일이 없었다. 그러나 2000년대 초반부터 인터넷을 이용한 기록저장, 온라인 대전 등을 지원하게 되었는데 이러한 점을 이용하여 네트워크 해킹을 통한 개인정보 유출, 테러 등등의 위험성이 생겼다. 이를 해결하기 위해서 각 회사마다 VPN을 도입하게 되었는데, 현재 이러한 서비스를 하는 곳은 KONAMI의 e-amusement[45], 세가 게임즈의 ALL.Net[46][47], 타이토의 NESiCA[48]가 있다.

이들은 각각 자신들의 서비스에 가입하고 기체를 구입할 때 VPN기기도 함께 제공한다. (외관은 유선 전용 공유기처럼

생겼다.) 그리고 VPN기기와 기체간 연결을 한 뒤 VPN기기와 모뎀을 연결하면 암호화된 정보로 본사 서버와 통신을 하여 네트워크에 연결이 된다. 기체를 많이 운영하는 오락실의 경우, 중간에 **스위칭 허브**를 두기도 한다. 그리고 보안성 향상을 위해 무조건 고정 IP를 사용한다. 만약 유동 IP를 사용하면 본사 서버에서 IP인증이 안 되어 네트워크 연결을 안 해준다.
상기한 이유로 보안성이 높기 때문에 몇몇 기체는 지원이 종료된 Windows 2000이나 Windows XP를 사용하기도 하며, 최근에는 Windows 7 embedded 또는 Windows 10 IoT를 탑재하기도 한다.

네오위즈와 누리조이도 비슷한 시스템을 운영하였지만 문제는 **VPN자체를 사용하지 않고 일반회선으로 평문통신**[49]으로 하고 있었다.🔗# 네오위즈의 경우 그래도 고정IP를 이용하지만 상기한 평문통신으로 인하여 계정 로그인[50]시 ID/PW가 쉽게 노출된다. 그러나 각각 DJMAX TECHNIKA와 BEATCRAFT CYCLON이 망하면서 사라졌다. 다만, 테크니카는 사설서버로 어찌어찌 명맥을 잇는 중. 안다미로의 AM.PASS역시 인트라넷이 아닌 일반회선에 연결되기 때문에 보안문제에서 벗어나기가 힘들다.

7.2. 온라인 게임에서의 이용

VPN 노드를 적절히 세팅하는 것으로 ISP들의 장난질을 방지할 수 있다는 점과, 직통 국제 해저 케이블 망을 거쳐가도록 유도할 수 있다는 점을 활용, 게임용으로 VPN을 사용하는 것이 가능하다. 한국에서는 회선 문제로 인해 핑이 튀는 현상이 잦아 이를 줄이기 위해 VPN으로 일본 등 주변국에 위치한 서버를 이용하여 레이턴시를 대폭 줄일 수 있다.

또한 e스포츠 대회용으로 사용되기도 하며, 대표적으로 각 국가 간의 핑 차이를 조절하기 위해 사용된다.

지역 제한이 걸린 일부 게임에서도 지역 제한을 우회하는 용도로 이용되기도 하며, 이 때문에 일부 게임 및 서비스에서는 이용 약관에 VPN 사용을 금지하는 조항이 있으므로 사용 시 주의가 필요하다.

7.2.1. 게임용 VPN 서비스

이외에도 게임용으로 설계된 VPN도 존재한다. 이들은 암호화를 거치지 않아 보안성과 익명성은 떨어지지만 속도는 매우 빠른 편이다.

다만 후술할 대표적인 게임용 VPN들의 서비스 품질이 영 좋지 않기 때문에[51] 일반 VPN들에 비해 메리트가 떨어지는 편이다. 대한민국에서는 영 좋지 않은 회선을 가지고 있을 때 효과를 볼 수 있으나, 대체로 게임용 VPN은 ISP들의 서버 상태가 좋지 않은 나라들이나, 미국 같이 국토 면적이 넓은 곳에서 사용된다.

- 미꾸라지 VPN - 가성비가 좋아 한국의 게이머들이 많이 이용하는 한국에서 개발된 게임용 VPN이다. 자세한 내용은 해당 문서로.
- WTFast - 게임용 VPN을 주력 사업으로 하는 캐나다 기업 및 그 서비스, ASUS 고급 공유기 등에 제휴 기능으로 들어가는 등 나름 입지를 넓히고 있다. 다만 스팀의 WTFast 관련 포럼에도 미꾸라지가 낫다는 평이 있는 등 미꾸라지와 직접적인 효과 비교에선 열위를 보이는 편이다. 이름의 유래는 다름 아닌 욕설 'What The Fuck'으로 추정된다.
- ExitLag

8. 프로토콜

- **PPTP** (Point to Point Tunneling Protocol)
  PPP(Point-to-Point Protocol) 기술을 확장하여 만든 규격이며, L2TP와 같이 PPTP도 터널을 확립해 주기만 하며, 암호화는 MS-CHAP와 RC4를 합성한다. 참고로 MS-CHAP는 마이크로소프트가 주도하여 만든 통신 규격이다. 대부분의 운영체제에서 기본적으로 지원하며, iOS에도 기본 내장되어 있**었**다. 안드로이드는 구글이 제작한 표준 규격에서는 기본 내장되어 있으나, 기종에 따라 내장 여부가 다르니 별도로 확인해 보자. 다만 이 규격은 시간이 지날수록 많은 보안상 결함이 발견되고 있으며, 애플의 경우 이 규격의 VPN에 연결하려 할 때 보안상 경고를 표시하기도 했다. 그러다 현재는 iOS 10및 macOS Sierra부터 PPTP를 아예 퇴출시킨 상태.[52] 안드로이드는 안드로이드 12 이후 퇴출됐다.🔗#

- **L2TP** (Layer 2 Tunneling Protocol)
  L2F와 PPTP 프로토콜을 결합하여 만든 규격이기 때문에 PPP를 지원한다. L2TP는 터널을 확립해 주기만 하며, 암호화는 IPsec 기술을 사용한다. IPsec 기술에는 IKE(Internet Key Exchange)와 ESP(Encapsulation Security Payload)가 사용된다. 해당 암호화 패킷을 차단하면 L2TP 규격을 사용할 수 없다. 대부분의 운영체제에서 기본적으로 지원하며, iOS에도 기본 내장되어 있다. 안드로이드는 구글이 제작한 표준 규격에서는 기본 내장되어 있으나, 안드로이드 12 이후 퇴출되었다.

- **OpenVPN**
  오픈소스 VPN이라는 뜻. **절대로 암호화가 안 돼서 OpenVPN인 것이 아니다.** TCP와 UDP 선택 연결을 사용한다. 기초규격은 L2TP를 따르지만, L2TP와 달리 세 개의 레이어를 확립할 수 있다는 특징이 있다. OpenVPN의 최대 장점은 프로파일 하나만 있으면 어떤 운영체제에서도 쉽게 연결할 수 있다는 점, 또한 VPN 장비나 공유기 없이도 VPN 서버를 설정할 수 있다는 점이 있다. 많은 OS를 지원하고 있으나 오픈소스라는 사정상 **내장되어 있지는 않다**. 허나 Android나 iOS 앱스토어에 공식 앱이 올라와 있으니 설치하고 프로파일만 끼얹으면 연결 잘 된다. 기숙사나 일부 교육기관처럼 VPN의 포트를 막는 경우가 종종 있는데, OpenVPN의 경우는 포트를 자율적으로 설정할 수 있고 일단은 공식적으로 포트를 할당받은 프로토콜이 아니기 때문에 VPN 막힌 곳에서도 잘만 쓸 수 있다는 장점이 있다. 또한 VPN 서버를 직접 구하는 방식이라, 무료 버전임에도 불구하고 매우 빠른 서버를 구하는 경우도 많다. 그러나 할당받은 프로토콜이 아니라는 점이 감지할 수 없다는 의미는 아닐뿐더러 정말 VPN을 작정하고 막는 경우 OpenVPN '정도는' 막아두기 때문에 근본적인 해결책은 되지 못할 수 있다.

- **SSTP** (Secure Socket Tunneling Protocol)
  SSL v3 규격을 사용하기 때문에 OpenVPN와 비슷한 장점을 지니고 있으며, 비교적 최근 만들어진 통신 규격이다. 마이크로소프트의 Windows Vista SP1에 추가되었으며, 현재 Linux와 다른 운영체제에서도 사용할 수 있다만 마이크로소프트가 SSTP를 소유하고 있기 때문에 아직까지는 Windows에 초점을 두고 있다. 또한 마이크로소프트가 NSA와 같이 운영한 것을 보고선 확실히 보안이 된다고는 할 수 없다.

- **WireGuard** (와이어 가드)
  WireGuard는 무료 오픈소스 소프트웨어 애플리케이션 및 통신 프로토콜이다. 이 프로토콜은 라우팅 되거나 브리지 된 구성에서 안전한 지점 대 지점 연결을 생성하기 위해 VPN 기법을 구현한다. WireGuard는 VPN 업계에서 시장의 판도를 바꾸는 제품이 될 수밖에 없다. 이 터널링 프로토콜은 최첨단 암호 기술과 매우 깔끔한 구조를 활용해 구축되었다. 따라서 다른 프로토콜보다 100배 적은 4,000줄의 코드만 있으면 비교적 쉽게 배포 및 감사, 버그 제거가 가능하며 일반적으로 OpenVPN 등의 기술보다 효율적인 동작이 가능하기에 공유기 등에 WireGuard 방식의 VPN을 구축 시 OpenVPN 대비 속도가 10~40% 가량 높아지는 경향을 보이며 핑 또한 소폭 낮아지는 경우를 많이 보여준다.
  이는 최적화 문제와 별개로 OpenVPN의 경우 싱글 스레드만 지원하지만 WireGuard는 멀티 스레드를 지원하는 영향이 더 크며
  2020년 3분기에 리비전된 WireGuard의 경우 100Gbps의 실질적인 처리를 위해 기존에 리비전1(4스레드) 리비전2(16스레드)까지만 이용하던 것을 리비전3 와서는 최대 64스레드까지 지원 가능하게 바뀌어 웬만한 게임보다 멀티스레드 이용률이 좋아졌다.

9. 구축용 소프트웨어

VPN 구축용 소프트웨어는 크게 사용자가 클라이언트만 구축하는 경우와 서버까지 직접 구축하는 경우로 나뉘며, VPN앱 또는 유료 솔루션등은 클라이언트만 구축하는 경우가 거의 다이다.
구축방법은 각종 커뮤니티에 잘 소개되어 있으니, 구글링을 하면 금방 나온다. 일부 소프트웨어는 나무위키에도 구축방법이 나와 있으니 각 문서들로.

서버까지 구축할 수 있는 솔루션을 제공하는 경우

- SoftEther VPN
- OpenVPN
- Outline
- Windows Server에 내장된 RRAS[53]
- Router OS
- 시놀로지 VPN Plus

클라이언트 솔루션만 제공하는 경우

- BlancVPN: https://blancvpn.com
- Hamachi
  IP를 우회하는 목적인 다른 VPN 프로그램과는 다르게 네이트워크 사용자끼리 연결된 일종의 인트라넷을 만들어 주는 형식이다.
- Hotspot Shield
- NordVPN
- Betternet
- ZenMate
- Wireguard
- 그 외 상용 SDN 소프트웨어[54]

10. 연결 방법

VPN서버로 연결하는 방법은 크게 두 가지로 나뉜다. 하나는 운영체제 자체의 기능을 통해 연결하는 방식이고, 두 번째는 자체 클라이언트를 통해 연결하는 방식이다. 운영체제 자체의 기능으로 이용하기 위해선 서버 주소와 서버 계정, 패스워드가 필요하다. L2TP의 경우엔 별도의 암호키나 암호 토큰이 추가로 필요하다. 경우에 따라 접속규격을 손봐줘야 하는 경우도 있다. 자체클라이언트의 경우는 클라이언트마다 전부 다르기 때문에 일일이 설명할 수 없으나, 대부분 원클릭으로 접속된다.

여기서 한 가지 주의할 점은, **유료 VPN**[55] 중에서 진짜로 VPN규격으로 접속하여 사용할 수 있는 VPN 서버는 **운영체제 자체의 기능으로도 연결할 수 있어야 한다.** 유료 VPN의 경우 접속할 수 있는 서버 주소와 당신의 계정이 공개되어 운영체제 자체의 규격으로도 접속할 수 있도록 한다. 만약 이러한 정보들이 하나도 공개되지 않고, 클라이언트로만 접속 가능한 유료 VPN이라면 200%의 확률로 겉에만 VPN이라고 써놓고, 까보면 프록시 서버거나 프록시 서버보다 못한 짝퉁이다.[56]

다만 예외로 운영체제 자체 기능이 아닌 경우 중에서 OpenVPN, Outline이나 클라이언트 자체에서 네트워크어뎁터를 제공하는 경우는 제외하도록 한다. 이는 오픈소스 계열 VPN이라서 상용 OS 측에서 자체 기능으로 편입시키기 애매하기 때문에 내장되어 있지 않는 거지, 분명 VPN이다. 다만 OpenVPN만 지원하는 유료 VPN은 극소수이긴 한데, 그 극소수 중 할인행사로 히트친 한 곳[57]이 있다.[58]

11. 장점

- 전용선을 일일이 끌어 쓸 필요가 없어서 장거리 통신망 구축비용이 매우 저렴하다.
- 전용선으로 연결된 컴퓨터가 아니어도 내부 네트워크에 접속할 수 있다.[59]
- 유튜브에 공식으로 올라온 한국 방송 하이라이트나 일부 일본 음악/애니메이션 PV를 볼 수 있다. 2014년 12월 1일부터 KBS와 EBS를 제외한 한국 방송사들이 동영상을 네이버 TV캐스트(현 네이버TV)나 다음 tv팟(현 카카오TV)에만 올리게 되면서 유튜브의 동영상을 한국 IP에 한해 차단하기 때문이다. 2015년 12월 27일부터는 KBS의 영상도 VPN을 이용해야 하며[60], 2016년 12월부터는 유튜브 레드(현 유튜브 프리미엄)의 한국 서비스로 인해 다수의 일본 레코드사가 관련 음악/애니메이션 PV의 재생을 차단했기 때문에 이 역시 VPN을 이용해야 한다.[61] 그러다가 MBC는 2017년 8월에 2000년대 중반까지의 방송분을 다시 정상 시청이 가능하도록 했다. 2019년 12월 21일부터는 모든 방송사에서 이 이후에 올라오는 영상들을 한국에서 시청 가능하게 했고, 그 전에 막아놨던 영상들도 다시 전부 풀렸다. 그 외에도 극소수이지만 특정 국가 법률에 위배되는 동영상[62]도 볼 수 있다.
- 외국 Play Store[63]나 App Store에 가입하거나, 외국 PayPal 서비스를 이용할 수 있다. 예를 들어, GTA 3부작의 10주년 기념 모바일버전은 한국 지역락이 걸려있어 한국에서는 구매가 불가능한데, VPN을 사용하면 미국 계정을 사용해 구매가 가능하다.
- 자신이 접속한 IP로는 이용이 불가능한 서비스 및 서비스 옵션을 이용할 수 있다. 예를 들어, 한국 IP에 한해서만 전면 유료화된 유튜브 뮤직을 무료로 이용하거나, 그 외에도 구글에서 성인인증 없이 모든 검색 결과를 노출시키거나[64], 유튜브에서 연령 제한 동영상을 성인인증 없이 시청하는 등으로 응용이 가능하다.
- 인터넷 검열과 지역 코드를 뚫고 자유로운 인터넷 사용이 가능해진다.[65] 중국이나 이란같이 서방 국가의 언론 및 SNS를 대부분 차단하는 국가의 거주자들은 아예 24시간 내내 VPN을 켜고 사는 사람들을 어렵지 않게 볼 수 있다.[66] 또한 검열로 막히지 않았어도 사이트 측에서 저작권이나 분쟁, 서비스 미제공 등을 이유로 특정 국가만, 또는 특정 국가가 아닌 곳에서의 접속을 차단하는 경우가 있는데, VPN을 사용하면 이러한 지역락이 걸린 사이트도 이용할 수 있다.
- 과거의 디즈니+와 같이 국가별로 다른 기간을 두고 서비스를 개시하는 OTT 서비스를 정식 런칭 이전에 이용할 수 있다. 혹은 아직 한국 진출 계획이 없는 OTT도 볼 수 있다.
- 서비스에 따라서는 VPN 접속을 공식적으로 막는 넷플릭스 같은 곳의 접속 제한도 집요하게 뚫어내어 거의 1년 내내 접속을 보장하는 근성을 보여주는 경우도 있다.

12. 단점

- 요금이 비싸다.[67]
- 타 국가의 서버를 거쳐서 접속하는 것이기 때문에 일반적인 인터넷보다 속도가 느려진다.[68]
- 전용선보다 상대적으로 보안에 취약하고[69] 인터넷 상황에 영향에 따라 서비스가 불가능할 수도 있다.
- 대한민국의 경우 실질적으로 사용할 수 있는 서버가 대한민국 외에는 대만, 홍콩, 마카오, 싱가포르, 일본, 미국, 캐나다, 영국, 프랑스, 독일, 호주, 뉴질랜드 정도밖에 없다. 그 이유는 아프리카, 남미의 서버는 지리적으로 멀어서 속도가 느리고, 상기의 제1세계 또는 서방 지역을 제외한 다른 지리적으로 가까운 인도 같은 서남아시아 서버의 경우, IT 인프라가 제대로 갖추어져 있지 않기 때문이고, 중국의 경우 말할 것도 없는 언론탄압으로 악명 높은 곳이다. 중국은 검열이 매우 심하고, 정보가 언제, 어디로, 어떻게 새어 나갈지 모르며, 그 서버를 제공하는 VPN 회사가 많지 않기 때문이다. 한편 대한민국 서버의 경우는 외국 유저가 주로 쓰고 자국민은 잘 쓰지 않지만, ISP가 외국계라면 검열 우회는 가능하다.
- VPN을 사용한 모욕 및 명예훼손의 경우 수사력의 부족으로 인해 증거불충분 또는 고소장 반려가 된다는 내용을 오독하여 대다수 국가에서 불법으로 규정하고 있는 성착취물 공유나 국가보안법 위반 등의 중죄까지 고소 및 고발되지 않는다고 믿는 네티즌들이 있으나, 단순 VPN 사용으로는 **모두 검거가 가능하다.** VPN 회사가 정말로 로그를 저장하지 않더라도 해당 국가의 인터넷 서비스 제공자(즉, 통신사)는 로그를 저장할 가능성이 높고, 설령 ISP가 로그를 저장하지 않는 법률이 제정된 나라의 서버를 이용하더라도 해당 나라에서 아청물 및 성착취물은 여전히 불법으로 규정될 가능성이 높기 때문에 선뜻 수사협조를 해줄 것이다. 그러면 입구와 출구를 동시에 장악한 수사기관이 접속 시간대와 패킷의 크기 등을 대조해 특정하는 게 가능해진다. 국가보안법의 경우 러시아, 중국, 홍콩 등 대한민국의 안보 이익을 공유하지 않는 나라의 서버를 사용할 경우 협조를 해주지 않을 것이라 생각할 수 있지만, 2022년 러시아의 우크라이나 침공 이후 러시아 VPN 서버는 전부 가상 서버로 바뀌었고 중국은 황금방패 때문

에 원래도 가상서버를 사용하고 있었다.

13. 악용

13.1. 스팸, 위키 반달 등 악용

스팸광고 및 위키에 반달리즘을 하는 데 악용하는 사용자들이 있다. 목적은 당연히 IP 세탁 및 IP 차단 회피용. 잦은 VPN 접속서버 변경을 통해 IP를 돌려가며 접속하는 방식으로 마치 여러 불특정 다수가 이용하는 것처럼 속일 수도 있다.

스팸광고 쪽은 이야기가 조금 다른데, 스팸을 올리는 작업장이 중국이나 다른 동남아 나라에 있는 일이 종종 있다. 따라서 속도 향상 및 IP 차단[70]을 뚫기 위해 국내 VPN을 사용한다. 국내 VPN 업체도 이런 수요가 있다는 것을 간파하고 "바이럴 마케팅용 VPN" 같은 이름으로 서비스를 제공하는 곳이 있다.

나무위키에서 발생한 상습 차단 회피의 반달 사례 중 상당수가 VPN을 이용한 악성 반달이다.[71]

때문에 대부분의 위키, 당근 등의 일부 웹사이트에서는 이러한 서비스 악용으로 인해 IDC 대역을 장기간 또는 무기한 차단으로 조치하고 있으나, NordVPN과 SurfShark 등의 유료 VPN 같은 경우는 대한민국 서버[72]를 제외한 해외의 모든 서버가 로그인 허용 차단으로 문서 편집이 제한적으로 가능하다. 2024년부터 나무위키의 경우 VPN 연결을 통한 문서 역사 및 이미지 보기 기능을 제한하는 조치를 취했으며, 2025년 11월 기준으로 사측에 의해 DataPacket(영국), M247(루마니아)[73] 회선을 사용하는 접속 및 열람도 전면 금지됐다.

13.2. 사기에 활용

사용자의 개인정보를 보호한다는 점을 악용한 사례로 물건/게임 아이템 거래 사이트를 주로 활용한다. 사기죄에서 행해지는 방법은 매우 단순하며 다음과 같다. 먼저, 물건을 판매한다는 글을 올린다. 구매 의사가 있는 사람이 등장하면 입금을 요구한다. 그다음에 잠수를 타거나 컴본갤 사례처럼 초코송이를 보내줘도 된다. 놀랍게도 이게 전부이다. 로그 기록을 제공하는 업체라면 잡을 수도 있겠지만[74] 많은 업체들이 No Log Policy 또는 Zero Log라는 이름으로 로그 저장 자체를 안 하는 경우가 있다. 이런 경우에는 잡기 힘들다. 그나마 계좌번호가 남아 있다면 추적이 가능하겠지만, 비트코인 송금이나 대리결제 등을 했다면 잡을 방법이 없다.[75] 더군다나 삼자사기에다 다른 사람의 대포폰이나 대포통장 등의 명의를 도용하였을 경우에는 잡아낼 방법이 없다.

13.3. 비방성으로 악용

한쪽에서는 언론 탄압을 해서 문제가 된다면 비방이나 모함을 해서 문제가 된다.

대한민국의 법률은, 명예훼손 또는 모욕(모욕죄)에 매우 엄격하다. 미국과는 달리 형사처벌까지 한다. 하지만 외국 VPN을 이용하여 **익명**으로 게시글, 댓글을 작성하면 피해자가 고소하려 해도 접수 자체를 안 받아 주는 경우가 많다. 고소를 한다고 해도 경찰서에서 '혐의없음(증거불충분)'이라고 적힌 통지서만 받게 될 것이다. 서버 로그를 지체 없이 발송해 주는 디시인사이드와는 달리 VPN 업체는 해외 지사라서 명예훼손이나 모욕으로는, 웬만해서는 수사 협조가 전혀 안 되기 때문이다. 당장 나무위키가 파라과이 법인임을 생각해 보자. 명예훼손, 모욕으로 실제로 조사를 받고 입건되는 자들은 자기 신상이 추적되었거나, VPN이 뭔지 모르거나, 1회성 VPN에 쓸 단돈 17000원의 자금도 없는 것이다.

운이 좋아서 vpn 업체 측의 협조를 받았다 해도 위의 경우처럼 서버 로그가 없다? NSA가 오지 않는 이상 잡을 수 없으며 NSA가 미국 법에 규정되어 있지 않은 명예훼손 및 모욕으로 힘을 빌려줄 일은 전혀 없다.[76] 이런 용도로 사용하기 적합한, 또 다른 소프트웨어 방법으로는 Tor가 있다.

디시인사이드같이 유동닉을 지원하는 인터넷 커뮤니티에서도 악성 유저들이 익명성 강화와 수사기관의 추적을 피하기 위해 Tor와 함께 악플 작성과 분탕 활동에 적극적으로 활용하고 있다. 2023년 대한민국 다발적 흉기난동 사태 이후로 디시에서 VPN을 포함한 해외 IP가 일괄적으로 차단되면서 덜해진긴 했지만, 끝내 막히지 않은 IP주소를 이용하는 경우는 있었고 이후 시간이 지나면서 해외 IP로도 다시 글작성이 기본적으로 가능해졌다.

다만 잘 모르면서 VPN 하나만 믿고 날뛰다가 망하는 경우가 있다. 바로 **한국** 업체나 무료 VPN을 쓰는 경우. 한국 업체가 VPN 서비스를 하는 경우, 만약 범죄 연루로 수사에 들어가는 순간 짤없이 한국법에 따라 수사에 협조해야 하기 때문. 그리고 무료 VPN의 경우 상술했듯이 이용자의 개인 정보를 수집해다 팔아넘기는 게 일과라서 그다지 보안을 기대할 수가 없다.

무엇보다 한국 사이트는 가입 시 실명 인증을 거쳐야 하는 이메일(네이버 메일, 카카오 메일 등)과 한국 전화 번호 인증을 요구하므로, 수사기관에서 IP주소 이외의 정보로도 사용자 신원을 특정할 수 있어서 VPN 사용 여부와 관계없이 고소가 가능한 경우가 대다수이다.[77]

13.4. 비정상적인 가격으로 제품 우회 구매

ESD 또는 서비스 업체는 국가별 물가와 환율 등을 고려하여 나라마다 다른 가격을 책정하는 경우가 많은데, 이때 VPN을 통해 터무니없이 싼 가격에 소프트웨어나 서비스를 구매하는 행위[78], 이른바 **VPN을 통한 부당한 우회 구매**도 문제시되고 있다. 베네수엘라판 윈도우 10을 구매하여 돈을 아끼려는 사람 때문에 터진 윈도우 10 대란과 스팀에서 러시아판 게임 구매로 돈 아끼려는 행위 등이 바로 그 사례이며, 이로 인해 해당 업계에선 골머리를 앓고 있다. 구글 또한 유튜브 프리미엄을 인도 VPN을 통한 우회 구매로 인해 피해를 본 전례도 있어 6개월 내에 해당 국가에 접속하지 않은 것이 확인되면 아예 프리미엄 혜택을 박탈하는 조치를 취하는 중이다. 이 때문에 해당 업계 상당수가 VPN을 통한 우회 구매를 지속적으로 무력화하는 등 피해를 최소화하고 있는 상황이다.

13.5. 그 외

자신이 게임에서 지속적으로 계정을 바꿔가면서 핵을 써서 IP가 차단을 당했음에도(또는 아예 VPN으로 다중계정 생성 후 VPN으로 핵을 이용) 다시 핵을 쓰고 싶어 IP 우회로 계정을 생성하려는 목적으로 VPN을 사용하는 경우가 있으며, 그렇게 되면 핵쟁이들의 폭주를 완전히 막을 수가 없어 애꿎은 정상 유저들이 피해를 보는 경우가 다반사이다.

2020년대 들어서 IP를 차단하면 지원되지 않는 국가에 거주하여 부득이하게 VPN을 사용하는 이용자들이 게임을 못하는 일이 발생하므로 약관 상에 VPN 사용 자체가 금지되어 있지 않는 이상 대부분 IP 차단까지는 하지 않는 추세이다. 그래서 일부 게임 회사들은 핵 사용자의 컴퓨터 메인보드 정보(HWID)를 기반으로 하드웨어 밴을 한다. 그러면 아무리 다중 계정을 만들어도 해당 컴퓨터 메인보드를 바꾸기 전에는 그대로 밴이 유지된다.

핵과 동급이거나 그 이상으로 악질적인 행위인 랜뽑~재연결(일명 lag switch)를 통한 게임 플레이 치팅에도 쓰인다. 일차적으로 연결되어 있는 VPN 서버 위치에서 커뮤니케이션이 되기 때문에 게임서버에서 플레이어의 연결상태를 확인하는 하트비트를 무력화하며, lag switch를 인위적으로 만들어낼 수 있다.

14. 기타

- 프록시 서버와 달리 가상 사설망은 개인적으로 서버를 돌리거나 단체여도 특수목적으로 쓰는 서버이기 때문에 무료로 접속이 가능한 가상 사설망은 자신의 집이 서버가 아닌 이상 거의 없다. 쉽게 접하는 무료 가상 사설망은 가상 사설망 서비스 업체가 제공하는 체험판인 경우가 대다수다.
- 리눅스 등에선 웹브라우저만 VPN을 연결해 쓸 수 있는 규격이 존재하지만. 윈도우에선 컴퓨터의 모든 프로그램이 가상 사설망 회선을 써야 한다. 물론 웹브라우저만 VPN을 연결해서 쓰게 할 수 있긴 한데, 이게 하필 VPN으로 연결되는 가짜 프록시 서버를 만들어서 쓰는 방법이라 대부분의 상용 VPN 서비스에서 사용이 불가능하고, 난이도도 매우 높다. 그나마 파이어폭스등 애드온이 존재하는 브라우저의 경우 브라우저 애드온들이 HTTP용 VPN을 제공하긴 한다. 그런데 정작 전문적인 상용 VPN 서비스들은 이런 애드온을 제공하지 않는다는 것이 함정. 방화벽

을 사용해서 특정 프로세스가 특정 네트워크만 사용하게 강제하는 것도 가능하긴 한데, 이 경우에는 프로그램마다 일일이 다 설정해 줘야 할뿐더러, 게임용 VPN을 같이 돌리는 경우와 같이 VPN을 두 개 써야 하는 경우에는 매우 곤란해진다. 이 경우에는 라우터의 포트 포워딩 기능을 이용해야 하는데, 역시 간단하지 않다.

- 쓰쿠바대학에서 무료로 제공하는 VPN Gate에서 자사 서비스 통계를 공개했는데 한국이 압도적으로 트래픽 1위를 찍고 있다. 사용량을 보면 알겠지만 대한민국, 이란, 러시아 등 인터넷 검열이 심한 국가들이 압도적이다.

순위	국가	트래픽	연결 수
1	대한민국	129,020,923.3 GB	586,568,079
2	이란	98,488,135.1 GB	5,310,407,635
3	러시아	87,795,715.5 GB	1,388,849,487
4	일본	67,454,021 GB	695,071,663
5	미국	52,592,078.1 GB	1,090,571,977
6	대만	50,344,245.1 GB	789,260,482
7	프랑스	46,084,272.1 GB	588,942,791
8	인도네시아	38,201,636.0 GB	888,644,804
9	인도	35,750,954.4 GB	768,664,451
10	중국	29,487,068.8 GB	771,177,178
2026년 5월 17일 기준			

사용자 수는 인구 대국이라 불리는 중국보다 1.4배 적은데 트래픽은 **4배 이상의 차이**가 난다! 이 정보는 실시간으로 갱신되고 있다. 🔗 랭킹 조회

- 몇몇 교육청들은 이와 관련된 사이트를 프록시 및 쇼크 사이트라 하면서 아예 접속을 막는다. 물론 VPN 서버의 주소를 막은 경우는 거의 없고, VPN 프로토콜을 차단하지도 않기에 일단 VPN을 다운로드하는 데 성공하면 자동적으로 뚫리게 된다.
- 일부 해외 게임에서는 접속하면 받을 수 없는 혜택도 받을 수 있다.
- 원래 VPN의 용도와 달리, 온라인 게임의 PC방 혜택을 집에서도 받기 위해 PC방 VPN으로 플레이하는 사람들이 있다. 이는 PC방의 이권을 엄청나게 침해하기 때문에, PC방에서 게임사에 압력을 강하게 넣는다.[79] 이를 의식해 대부분의 게임사에서는 발견 즉시 계정 영구정지 조치를 취하고 있다. 때문에 지금은 많이 사라졌지만 간간히 운영되는 곳이 있는 듯하다. 다만, 이런 회사들은 정식으로 사업자 등록을 하고 게임사에 돈을 내며 프리미엄을 받아오는 등 나름 합법적으로 운영하고 있기 때문에 법적인 단속은 힘들다.[80]
- 스팀 등 일부 ESD 플랫폼에서는 VPN을 통한 우회 구매는 약관상 금지되어 있으며, 적발될 경우 최악의 경우 계정 블럭까지 먹을 수 있다.[81] MS와 구글의 경우는 VPN을 통한 우회 구매를 아예 무력화하는 방법으로 차단하는 중이다.
- VPN 회사에게 돈 받고 뒷광고하는 블로거들이 많다고 한다. 그나마 유튜버들의 경우, 특히 해외 유튜버들은 정식으로 스폰서 광고임을 밝히는 경우가 많으므로 크게 문제 되지 않지만, 그 외의 곳에서는 아주 심각하다. 무엇보다 **당신의 개인정보를 감시로부터 보호하고 안전한 인터넷 접속을 보장받고 싶으시다면** 같은 상투적인 문구가 절대로 빠지는 일이 없는 VPN 홍보를 스폰서 광고가 아니라고 포장하는 일이 더 어려울지도 모른다. 심지어 VPN 회사 광고가 저작권 우회를 직접적으로 알려주는 업체가 있어 기업 간 마찰이 생기기도 한다.[82]
- 해외 법인의 회사들이 규모가 커지면서 한국 지사 역시 많아지고 있다.

15. 같이 보기

- Tor
- 인터넷 프라이버시

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.